Educational Supply Chain for Dependable Software

US Software Assurance Forum – Fall 2011
15 September 2011 – Arlington VA US

[DMU/CSC/SSDR/2011/092 | v1.0 | 20110915]

Ian Bryant
Technical Director
Software Security, Dependability and Resilience

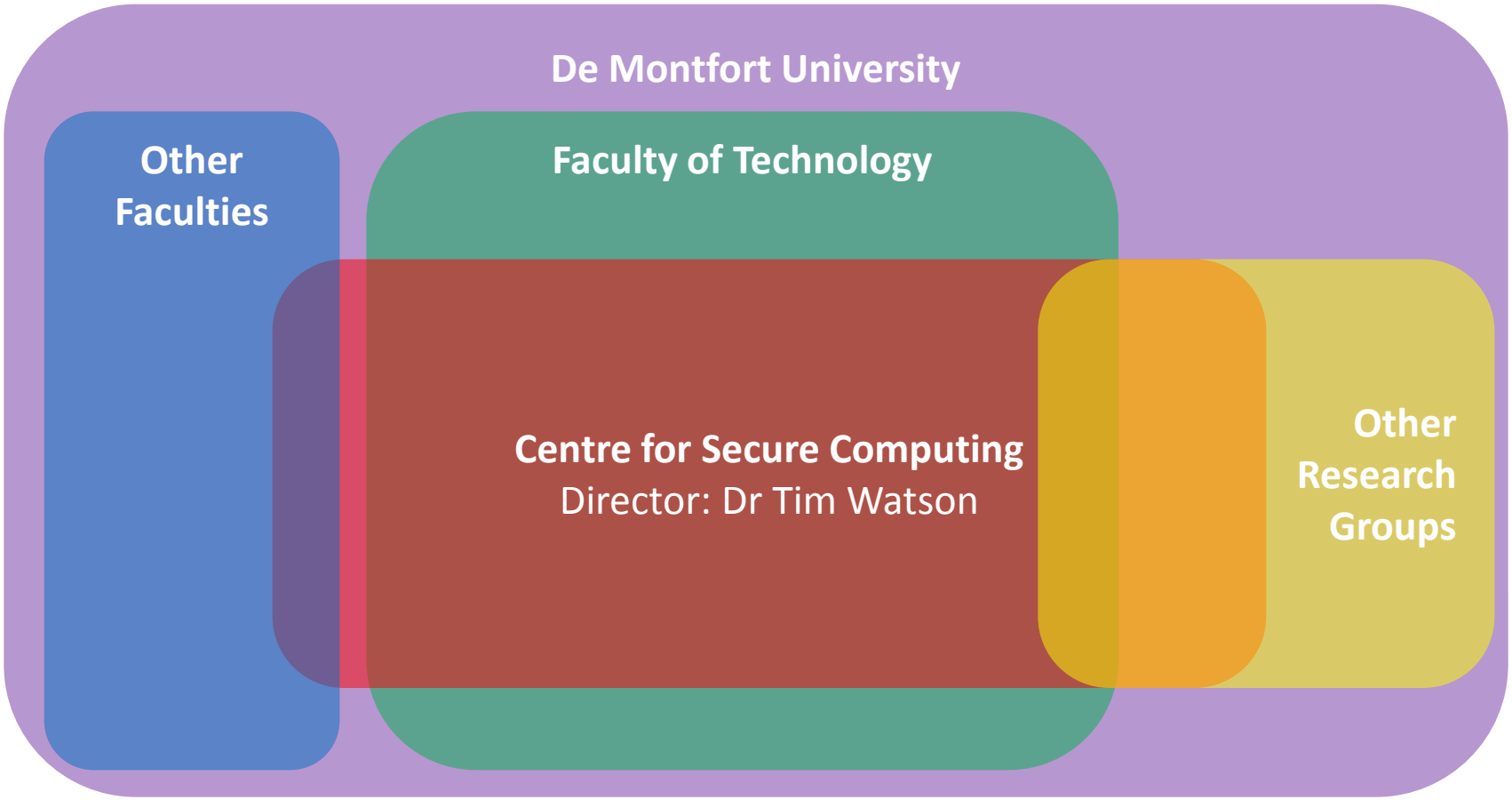
Educational Supply Chain for Dependable Software

- About DMU CSC
- The Challenges
- Thoughts on T E A
- Education for Dependable Software
- SSDRI
- Questions?

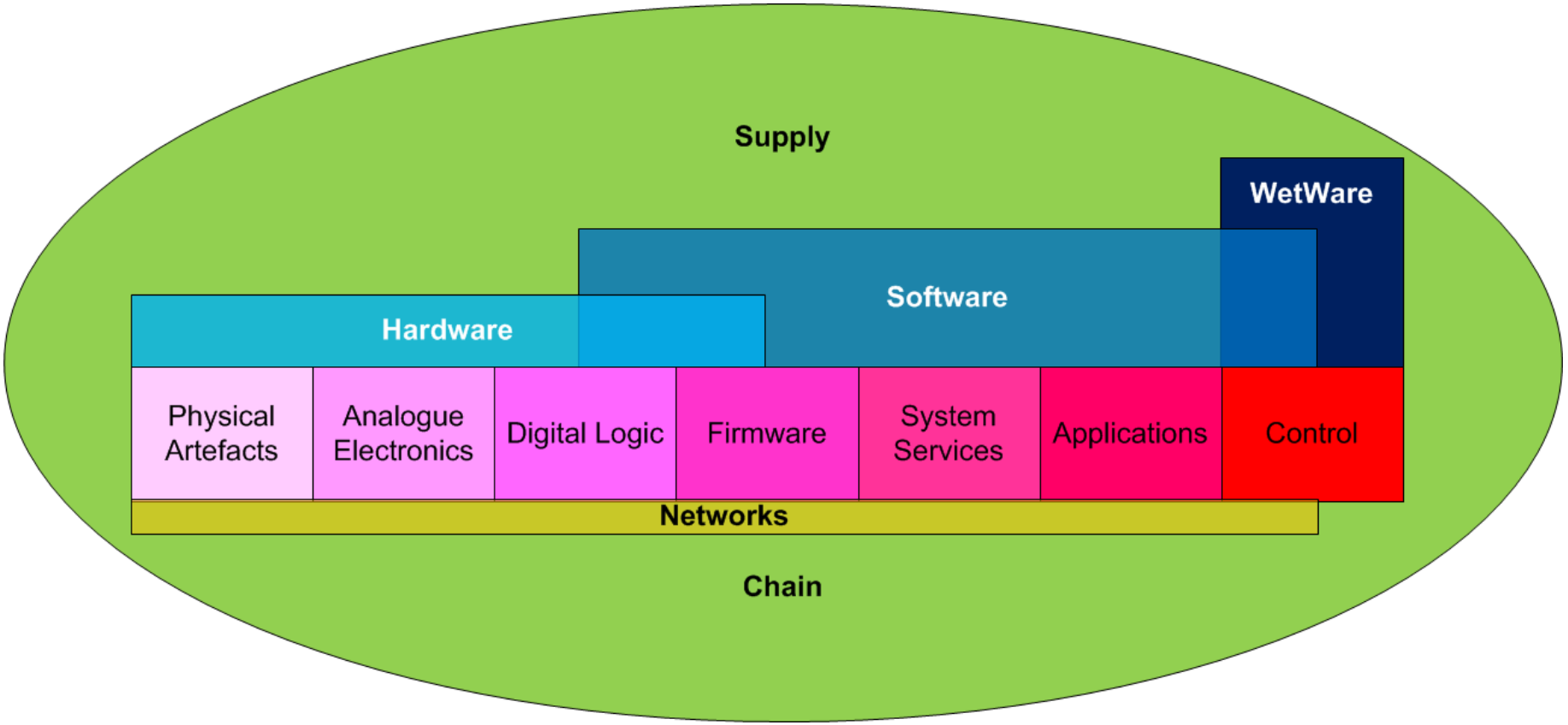
De Montfort University (DMU)

- One of the highest performing modern “Alliance” Universities for research, with its academic excellence proven by latest Research Assessment Exercise (RAE) 2008, showing nearly half of its research to be ‘internationally excellent’ or ‘world-leading’
- The Faculty of Technology has an international standing and has achieved 4-star ratings in the Research Assessment Exercise (RAE)
- The **Centre for Secure Computing (CSC)** is a newly formed Research Centre, within the Department of Computer Technology, focusing on the sort of cross-functional projects that gives De Montfort its distinctiveness by working in a matrix style across multiple Departments and Faculties

Secure Computing at DMU



Challenge Area: What is Software ?



Challenge Area: What is Cybersecurity?

- Cybersecurity is the emergent, *de facto* term for the holistic protection of information in an Information and Communications Technology (ICT) context
- It can be considered to be an extension of Information Security , with the following 3 extensions :
  - Dependencies upon, and controls to interact with, infrastructure providers and other Alerting, Warning and Response (AWR) functions
  - Enhanced Proactive IA controls and capabilities to detect events and reduce impacts
  - Enhanced Reactive IA controls and capabilities, both to maintain situational awareness and, where applicable, instigate active response (e.g. arrest of suspects)

Challenge Area: Development

- Underlying assumption software will be developed under engineering-style “waterfall” model, under single organisational control
- Challenges to these assumptions include:
  - Agile Development
  - Open Source
  - Untrusted platforms (incl. counterfeit hardware)
  - Software / hardware boundary (e.g. VDHL)
  - Multicore Processors

Challenge Area: Adversities

- Few practitioners treat Adversity
- Information Security community address Threat
  - Deterministic model with problems handling Known, Unknown and Unknowable (KuU) factors
  - Often ignores Hazards
- System Reliability / Safety community address Hazards
  - Typically Stochastic model
  - Approach usually ignores Threat

Challenge Area: Evolving Environment

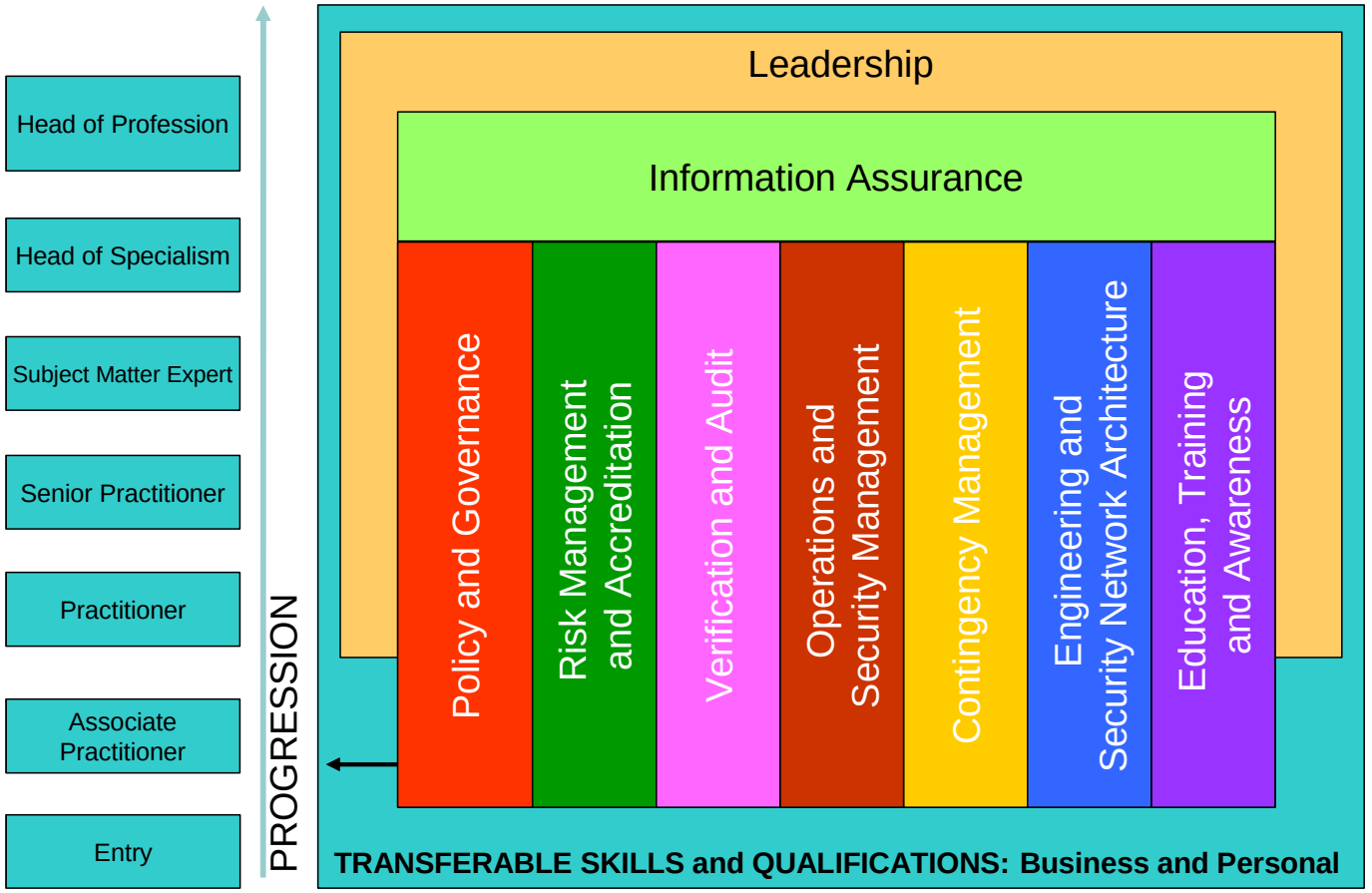
- 2010 UK National Security Strategy has Cyber-attack and deficiencies as one of the 4 “Tier One” Risks
- New Technological / Societal challenges:
  - Distributed application platforms and services (“Cloud”)
  - Mobile Devices and Lightweight operating systems
  - Consumerisation / Bring-Your-Own-Device (BYOD)
  - Commoditisation in previously closed architectures
  - Consolidation for energy efficiency (Low Carbon / Green)
- These are likely to present Disruptive Challenges, fundamentally deepening dependence on Software

A Very British Answer - T E A

T E A

- **Training**
  - Updating and/or re-skilling the current practitioner base
- **Education**
  - **Preparing the future workforce**
- **Awareness**
  - Backdrop for all Stakeholders
    - Demand-side
    - Supply-side
    - Those producing the Corpus of knowledge

Cybersecurity Specialism Matrix



Source: General Information Assurance (IA) Products and Services Initiative: IA Competency Framework

Cybersecurity Practitioner Roles

- Senior Leadership
- Policy and Governance
- Risk Management & Accreditation
  - Risk Analysis, Risk Assessment, Accreditation
- Verification and Audit
  - Evaluation, PenTest, Forensics, Audit
- Operations and Security Management
  - Network/Systems Security Officers, Physical / Personnel Security, Crypto Custodians, Operators, System Administrators, Information Managers
- Contingency Management
  - CSIRT, WARP, BCP
- **Engineering and Security Network Architecture**
  - **Design, Development, Implementation**
- Education, Training and Awareness

Targets of Delivery

- Practitioners community is not monolithic:
  - Cybersecurity specialists
  - Other ICT disciplines
  - Other related disciplines
- In addition to dedicated training for Cybersecurity specialists, goal should be for all Undergraduate level courses in relevant training to have a Awareness element on topics like Software Security, Dependability and Resilience

Modular Cybersecurity Curriculum

- All practitioners should be educated in a Mandatory Core that applies across the Cybersecurity realm
- For each area of specialism, Packaged Curricula need to be established by assembly of relevant elective units at
  - Introductory level
  - Advanced level
  - Applied level

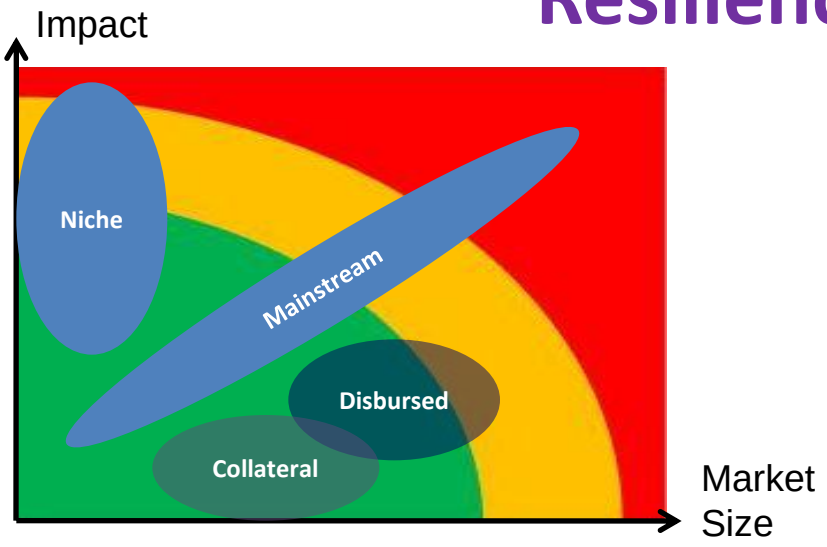
Mandatory Cybersecurity Core Curriculum

- Asset Utility as applied to both Information and to ICT Systems
- Adversities (Threats and Hazards)
- Vulnerabilities and Weaknesses
- ICT Systems Architecture
- Control Techniques and Options
  - Personnel
  - Physical
  - Procedural
  - Technical

Packaged Cybersecurity Curricula Modules

- **Acquisition**
- **Data and Information Security**
- **Digital Forensics**
- Enterprise Continuity
- Incident Management
- Information Risk Management
- ICT Systems Operations and Maintenance
- Network and Telecommunications Security
- Personnel Security
- Physical and Environmental Security
- **Regulatory and Standards Compliance**
- ➢ **Software Security, Dependability and Resilience**
- Strategic Cybersecurity Management
- Training and Awareness

Software Security, Dependability and Resilience Initiative (S S D R I)



Capability

- **Making Software Better:**
- *"Enhancing the overall software and systems culture, with the objective that all software should become designed, implemented and maintained in a secure, dependable and resilient manner"*

Activities

- ➢ **WP1: Environmental Shaping**
- WP2: Conceptual Evolution
- ➢ **WP3: Practice Development**
- (*WP4: Independent Verification*)
- WP5: International Collaboration
- WP6: Standards Contribution

Delivery

- **Approach:** A public-private initiative, encompassing both the Demand- and Supply-side communities, and those producing the Corpus of knowledge
- **Technical Director:** Ian Bryant (ian.bryant@ssdri.org.uk), DMU CSC
- **Milestones:** Launched 1st July 2011

SSDRI Special Interest Groups (SIG)

- Main vehicle for SSDRI delivery of its remit for producing a harmonised, UK view of the various subject areas will be through Special Interest Groups (SIG)
- SIGs formed of *pro bono* technical contributors from across all sectors of UK economy
- List of SIGs currently still being defined, but draft set of 10 is:

- Rationale
- **Awareness**
- Metrics
- **Guidance**
- Supply Chain Risk Management
- **Education**
- **Training**
- Standards
- Conceptual Evolution
- Verification and Testing (*for WP4: In Abeyance*)

SSDRI: Awareness

- SSDRI aims to produce a harmonised, UK view of the various subject areas within its remit
- Channels for dissemination include:
  - SSDRI Website (**www.ssdri.org.uk**) – to become "one stop shop" for information – including links to off site Normative References
  - News Feed (on Twitter **@ssdriuk**)
  - Softcopy or hardcopy deliverables (website and/or Channel Partners)
  - Courseware as used by Education / Training Channel Partners
  - Outreach activities, including Presentations and Conference Papers
- Other deliverables will include contributions to Standards
- Timescales for availability of material will vary
  - Some "Quick Wins" will be on website within 1st year
  - Long-term / strategic items will unavoidably take several years to reach maturity (e.g. Standards)

SSDRI: Training - Supply-side Segments

- **Mainstream**
  - "The Industry" e.g. Microsoft, Oracle, ...
- **Niche**
  - Specialist Industries e.g. Aviation, "Security"
- **Disbursed**
  - Small scale developers e.g. SmartPhone Apps
- **Collateral**
  - Developers don't consider themselves as such
  - e.g. Embedded systems, website CMS Users, spreadsheets, …

UK/US Collaboration

UK (SSDRI) Special Interest Groups (DRAFT [1])	US (BSI / SwA) Working Groups
Rationale	Business Case
Awareness	-
Metrics	Measurement
Guidance	Processes and Practices
Supply Chain Risk Management	Acquisition and Outsourcing [2]
Education	Workforce Education and Training
Training	
Standards	-
Conceptual Evolution	Technology and Tools
Verification and Testing [3]	
-	Malware

[1] This list of SIGs can be expected to be, at least partially, dynamic
[2] Linked to DOD activity in Supply Chain Risk Management (SCRM), which includes links into hardware realm such as anti-counterfeiting
[3] For WP4 (Independent Verification) – currently in abeyance

Any Questions ?

Contact Details

Ian Bryant

Technical Director SSDR

Centre for Security Computing

De Montfort University

The Gateway, Leicester, LE1 9BH, England

ib@dmu.ac.uk; Internet

+44 79 7312 1924; Mobile

http://www.dmu.ac.uk/